Visual Algebra

Lecture 2.1: Complex numbers and matrices

Dr. Matthew Macauley

School of Mathematical & Statistical Sciences
Clemson University
South Carolina, USA
http://www.math.clemson.edu/~macaule/

Families of groups

In the previous chapter, we encoutered groups meant to appeal to intuition and motivate key concepts. In this chapter, we'll introduce a number of families of groups.

We'll need a diverse collection of go-to examples to keep us grounded. We'll begin with

1. **cyclic groups**: rotational symmetries
2. **abelian groups**: $ab = ba$
3. **dihedral groups**: rotational *and* reflective symmetries
4. **permutation groups**: collections of rearrangements.

We'll show that *every* finite group is isomorphic to a permutation group.

Then, by modifying some of our familiar groups, we'll encounter the:

5. **quaternion** and **dicyclic groups**,
6. **diquaternion groups**
7. **semidihedral** and **semiabelian groups**.

Finally, we'll take a tour of:

8. **groups of matrices**
9. **direct products** and **semidirect products** of groups.

We'll see a few other visualization techniques and surprises along the way.

A few basic definitions

We'll study subgroups in Chapter 3, but it's helpful to formally define this concept now.

Definition

A **subgroup** of G is a subset $H \subseteq G$ that is also a group. We denote this by $H \leq G$.

Definition

The **order of a group** G is its size as a set, denoted by $|G|$.

Definition

The **order of an element** $g \in G$ is $|g| := \big|\langle g \rangle\big|$, i.e., either

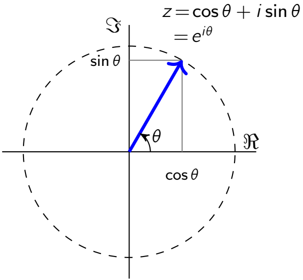
- the minimal $k \geq 1$ such that $g^k = e$, or
- ∞, if there is no such k.

A few basic definitions

The complex numbers are the set

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}, \qquad \text{where } i^2 = -1.$$

By Euler's identity, $e^{i\theta} = \cos\theta + i\sin\theta$ lies on the unit circle.



From this, we get the polar form:

$$z = a + bi = Re^{i\theta}, \qquad \tan\theta = b/a.$$

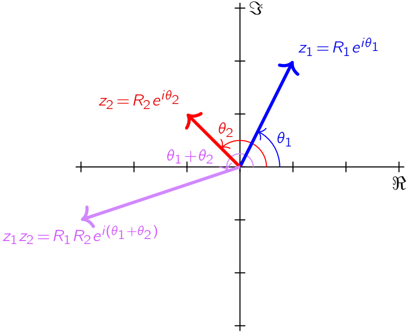
The norm of $z \in \mathbb{C}$ is $|z| := R = \sqrt{a^2 + b^2}$.

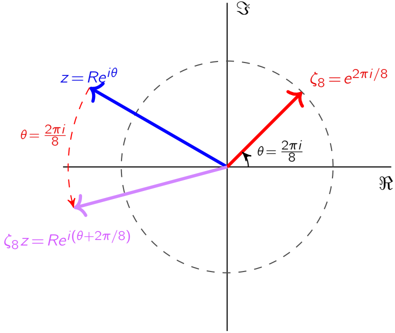
Remark

If two complex numbers are multiplied, their lengths multiply and their angles add.

$$z_1 = R_1 e^{\theta_1}, \quad z_2 = R_2 e^{\theta_2} \qquad \Longrightarrow \qquad z_1 z_2 = (R_1 e^{i\theta_1})(R_2 e^{i\theta_2}) = R_1 R_2 e^{i(\theta_1 + \theta_2)}.$$

Review of complex numbers





The complex conjugate of $z = Re^{i\theta} = a + bi$ is

$$\overline{z} = Re^{-i\theta} = a - bi,$$

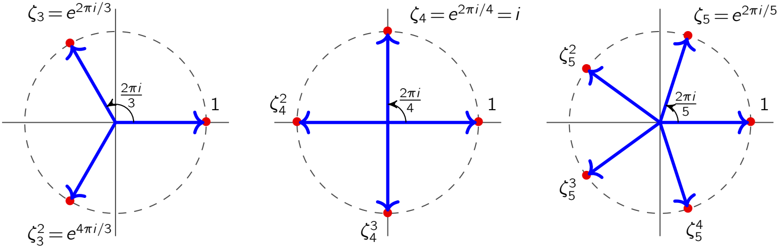
which is the reflection of z across the real axis.

Note that

$$|z|^2 = z \cdot \overline{z} = Re^{i\theta}Re^{-i\theta} = R^2 e^0 = R^2 \quad \Longrightarrow \quad |z| = \sqrt{z\overline{z}} = \sqrt{a^2 + b^2} = R.$$

Roots of unity

The polynomial $f(x) = x^n - 1$ has n distinct roots, and they lie on the unit circle.



Definition

For $n \geq 1$, the n^{th} roots of unity are the n roots of $f(x) = x^n - 1$, i.e.,

$$U_n := \{\zeta_n^k \mid k = 0, \dots, n-1,\ \zeta_n = e^{2\pi i/n}\}.$$

If $\gcd(n, k) = 1$, then ζ_n^k is a primitive n^{th} root of unity.

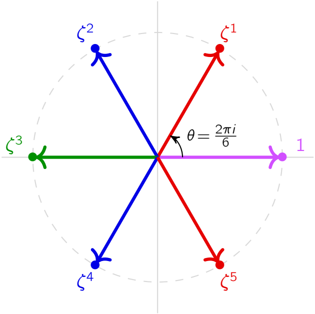
Remark

The n^{th} roots of unity form a group under multiplication.

A motivating example: the 6^{th} roots of unity

The 6^{th} roots of unity are the roots of the polynomial

$$\begin{aligned} x^6 - 1 &= (x-1)(x^5+x^4+x^3+x^2+x+1) \\ &= (x-1)(x-e^{2\pi i/6})(x-e^{4\pi i/6})(x-e^{6\pi i/6})(x-e^{8\pi i/6})(x-e^{10\pi i/6}) \\ &= (x-1)(x+1)(x^2+x+1)(x^2-x+1) \\ &= \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) \end{aligned}$$



- $\zeta^0 = e^{0\pi i/6} = 1$: primitive 1^{st} root of unity
- $\zeta^1 = e^{2\pi i/6} = \frac{1}{2} + \frac{\sqrt{3}}{2}i$: primitive 6^{th} root of unity
- $\zeta^2 = e^{4\pi i/6} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$: primitive 3^{rd} root of unity
- $\zeta^3 = e^{6\pi i/6} = -1$: primitive 2^{nd} root of unity
- $\zeta^4 = e^{8\pi i/6} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$: primitive 3^{rd} root of unity
- $\zeta^5 = e^{10\pi i/6} = \frac{1}{2} - \frac{\sqrt{3}}{2}i$: primitive 6^{th} root of unity

Do you see how this generalizes for arbitrary n?

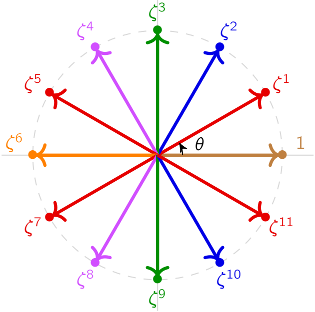
Cyclotomic polynomials

The n^{th} cyclotomic polynomial is $\Phi_n(x) := \prod_{\substack{0 \leq k < n \\ \gcd(n,k)=1}} (x - e^{2\pi i k/n}) = \prod_{\substack{0 \leq k < n \\ \gcd(n,k)=1}} (x - \zeta_n^k)$.

That is, its roots are precisely the primitive n^{th} roots of unity.

An important fact from number theory is that $\Phi_d(x)$ is irreducible and $x^n - 1 = \prod_{0<d \mid n} \Phi_d(x)$.

$$x^{12} - 1 = \Phi_{12}(x)\,\Phi_6(x)\,\Phi_4(x)\,\Phi_3(x)\,\Phi_2(x)\,\Phi_1(x)$$
$$= (x^4 - x^2 + 1)(x^2 - x + 1)(x^2 + 1)(x^2 + x + 1)(x + 1)(x - 1)$$



- primitive 12^{th} roots of unity: ζ^1, ζ^5, ζ^7, ζ^{11}
- primitive 6^{th} roots of unity: ζ^2, ζ^{10}
- primitive 4^{th} roots of unity: ζ^3, ζ^9
- primitive 3^{rd} roots of unity: ζ^4, ζ^8
- primitive 2^{nd} root of unity: ζ^6
- primitive 1^{st} root of unity: $\zeta^0 = 1$.

Remark

Primitive d^{th} roots of unity: $\{\zeta^k \mid \gcd(n,k) = n/d\}$.

Reflection matrices

The roots of unity are convenient for representing rotations, but not reflections.

A 2×2 real-valued matrix A is a linear transformation

$$A\colon \mathbb{R}^2 \longrightarrow \mathbb{R}^2, \qquad \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} ax+by \\ cx+dy \end{bmatrix}.$$

A reflection across the x-axis (i.e., $v \in V_4$) is the map $(x, y) \mapsto (x, -y)$.

A reflection across the y-axis (i.e., $h \in V_4$) is the map $(x, y) \mapsto (-x, y)$.

In matrix form, these are

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ -y \end{bmatrix}, \qquad \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -x \\ y \end{bmatrix}.$$

Multiplying these matrices in either order is $-I$, which is the map $(x, y) \mapsto (-x, -y)$:

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -x \\ -y \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}.$$

Mathematically, this is a representation of the group V_4:

$$V_4 \cong \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \right\}.$$

Rotation matrices

For $\theta \in [0, 2\pi)$, the rotation matrix

$$A_\theta = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$$

is a counterclockwise rotation of $\mathbb{R}^2$ about the origin by θ.

Rotating by θ_1 and then by θ_2 is a rotation by $\theta_1 + \theta_2$. Algebraically,

$$A_{\theta_1} A_{\theta_2} = A_{\theta_1 + \theta_2}.$$

Recall that multiplication by $e^{2\pi i/n}$ is a counterclockwise rotation of $2\pi/n$ radians in $\mathbb{C}$.

In terms of matrices, this is multiplication by

$$A_{2\pi/n} = \begin{bmatrix} \cos(2\pi/n) & -\sin(2\pi/n) \\ \sin(2\pi/n) & \cos(2\pi/n) \end{bmatrix}.$$

We can also represent rotations with complex matrices:

$$R_n := \begin{bmatrix} e^{2\pi i/n} & 0 \\ 0 & e^{-2\pi i/n} \end{bmatrix} = \begin{bmatrix} \zeta_n & 0 \\ 0 & \overline{\zeta}_n \end{bmatrix}.$$